Automation in Transportation Accidents

Deborah Bruce

National Transportation Safety Board

Washington, DC

Automation Accidents

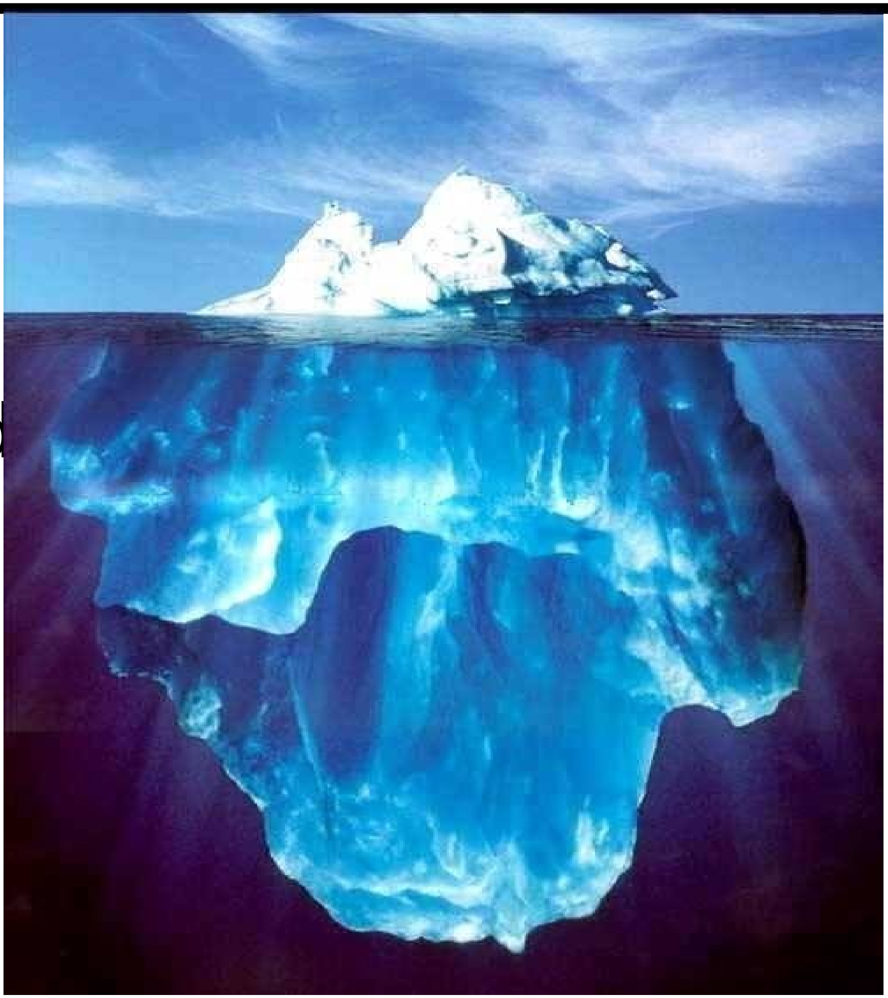
Control System Design

AUTOMATION ACCIDENTS
occur when there is a disconnect between the control system and operator

Person
- Monitoring
- Task overload
- Expectancy
- Inattention
- Complacency
- etc...

The Role of Automation

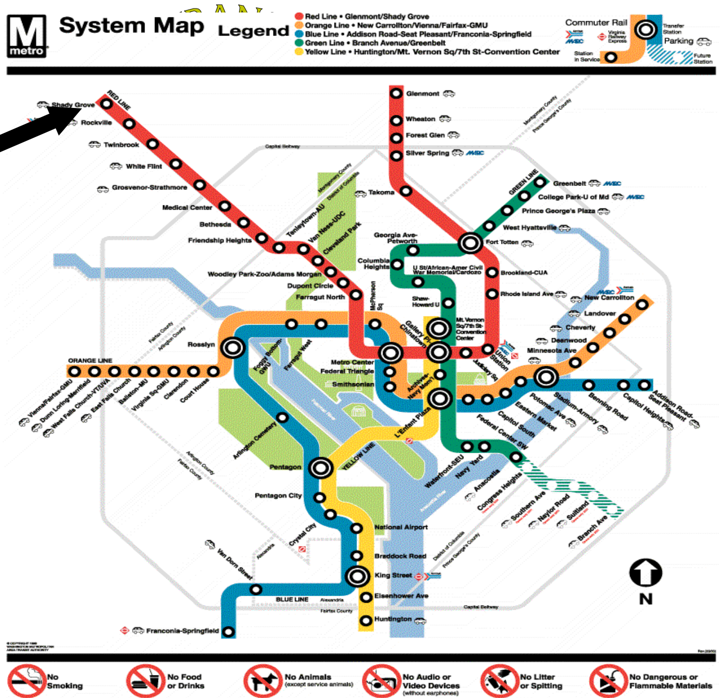
- Transportation databases focus on fatalities
- Automation-related mistakes difficult to analyze
- Varied and inconsistent taxonomies



Accident Examples

- Washington Metro Train Collision
  - Shady Grove MD on Jan 6, 1996
- Grounding of the Royal Majesty
  - Near Nantucket on June 10, 1995
- Pipeline release of hazardous liquid
  - Near Gramercy LA on May 23, 1996
- A300 Inflight Upset
  - Near West Palm Breach FL on May 12, 1997

Metro train


metro
System Map
Legend
Red Line • Glenmont/Shady Grove
Orange Line • New Carrollton/Vienna/Fairfax-GMU
Blue Line • Addison Road-Seat Pleasant/Franconia-Springfield
Green Line • Branch Avenue/Greenbelt
Yellow Line • Huntington/Mt. Vernon Sq/7th St-Convention Center
Commuter Rail
Transfer Station
Parking
Station in Service
Future Station
Shady Grove
Rockville
Twinbrook
White Flint
Grosvenor-Strathmore
Medical Center
Bethesda
Friendship Heights
Glenmont
Wheaton
Forest Glen
Silver Spring
Takoma
Greenbelt
College Park-U of Md
Prince George's Plaza
West Hyattsville
Fort Totten
Brookland-CUA
Rhode Island Ave
New Carrollton
Landover
Cheverly
Deanwood
Minnesota Ave
Rosslyn
Pentagon
Pentagon City
National Airport
Braddock Road
King Street
Eisenhower Ave
Huntington
Franconia-Springfield
RED LINE
GREEN LINE
ORANGE LINE
BLUE LINE
YELLOW LINE
N
No Smoking
No Food or Drinks
No Animals (except service animals)
No Audio or Video Devices (without earphones)
No Litter or Spitting
No Dangerous or Flammable Materials

Pre-Accident Events

- Severe snow storm track conditions worsening.
- All Metrorail trains were functioning in Automatic train operation as opposed to Manual operations.
- Computerized system at Metro’s Operations Control Center controls train acceleration, speed, and braking.
- Train operator responsible primarily for monitoring train functions and ensuring safe operations.

Metrorail Operations Control Center

- Controllers monitor and direct operations throughout the system.
- Controllers set parameters for trains by assigning the train’s “performance levels” (train’s acceleration and top speed).
- Under new Metro policy, controllers were not permitted to authorize train operators to change from automatic to manual mode except in emergencies.

Metro Operating Practices

- High number of wheel flats on Metro train . . . because of braking slides in manual mode.
- The November 17, 1995, notice instructing controllers *not* to permit train operators to change to manual mode (except in emergencies).
- The Jan. 6, 1996 storm was the first serious snow storm after change - - first real test of the new policy.

Accident Sequence

- Controllers instructed the train to continue Automatic mode, set speed at lower performance level (59 mph).
- Train overruns Twinbrook Station (told by controllers not to service station go to next in Automatic mode).
- The train then overran Rockville Station by one car. Results in *performance level* loss because the train was not within platform limits.
- Thus, the train departed to Shady Grove Station at 75 mph (rather than 59 mph). Train overran station by 470 ft, struck and telescoped 21 feet into standing train.

NTSB Findings

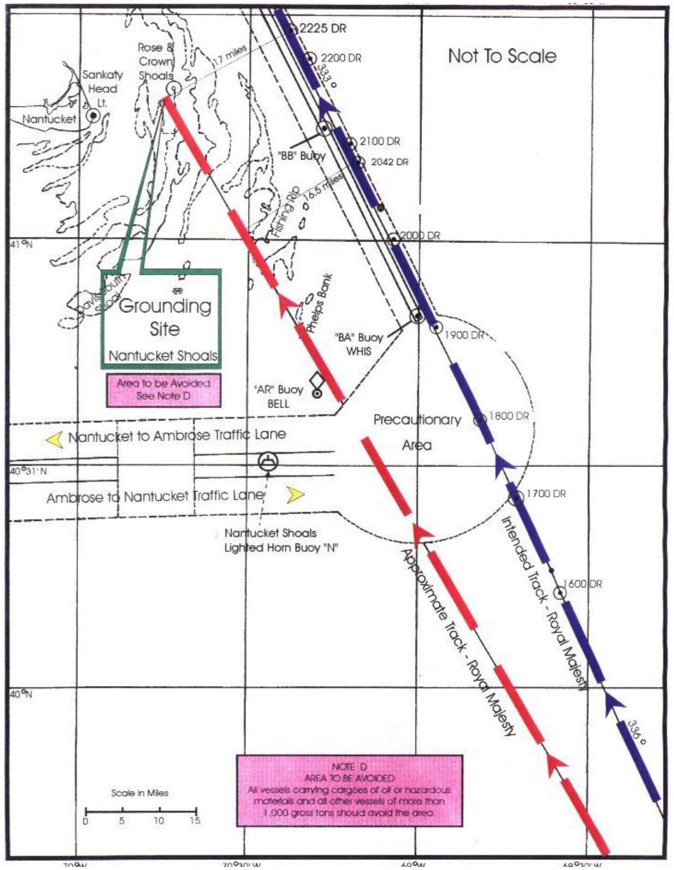
- Safety Board found over reliance on system automation to ensure safe train operations.
- Controllers had responsibility for day-to-day train operations, but lacked authority.
- For the 20 year history of Metrorail, controllers routinely gave permission for train operators to change to manual operation during periods of inclement weather.
- Controllers felt that train operator could do a better job of controlling the trains manually in slippery track conditions.

NTSB Conclusions

- Metro management practices were inconsistent with complex automated rail system.
- Decisions for highly technical automated systems usually affect other activities (and sometimes produce unanticipated hazards).
- Metrorail management failed to fully understand the design features and limitations of the automatic train control system--
- Which led to unjustified management confidence that the system could ensure safe train operation under all operating conditions.

Royal Majesty

Navigational Track



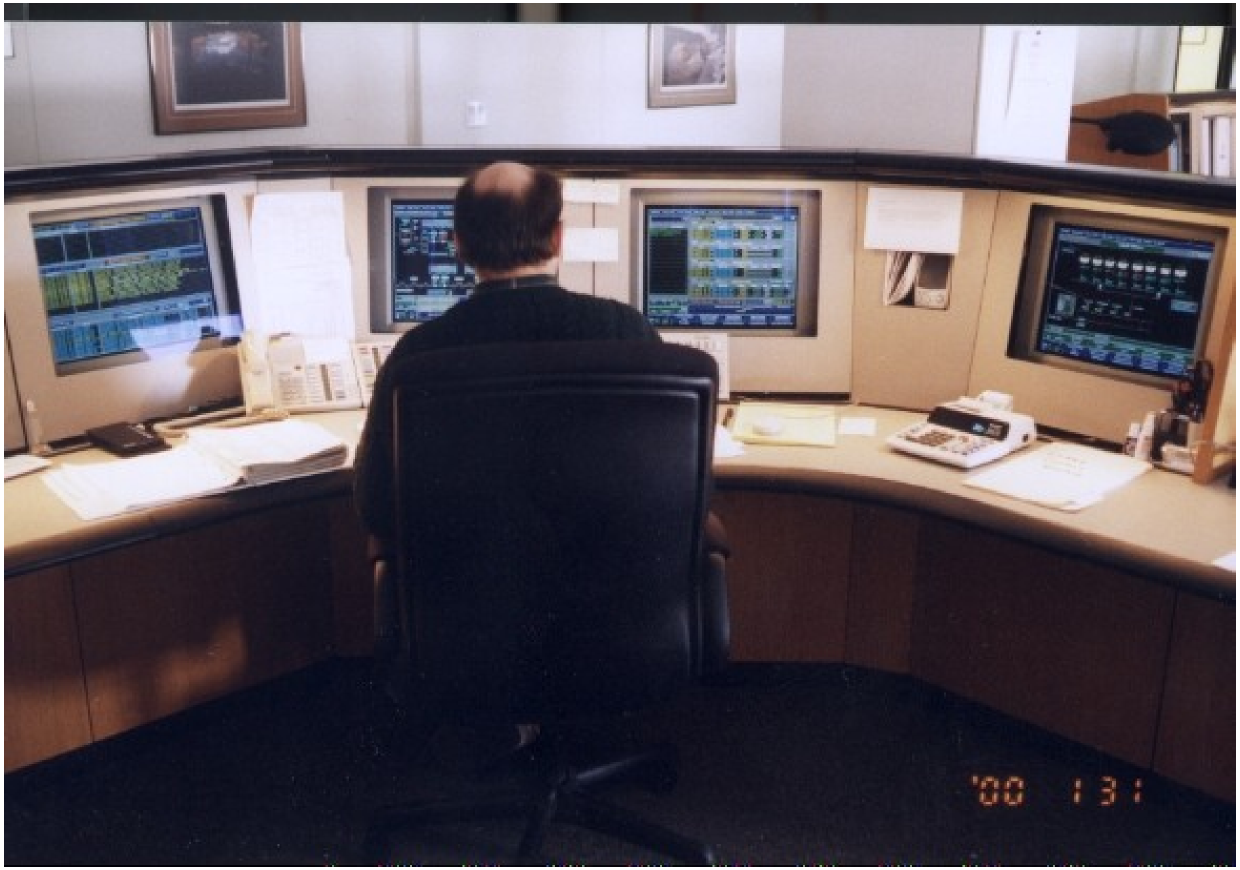
Integrated Control Bridge

Chartroom

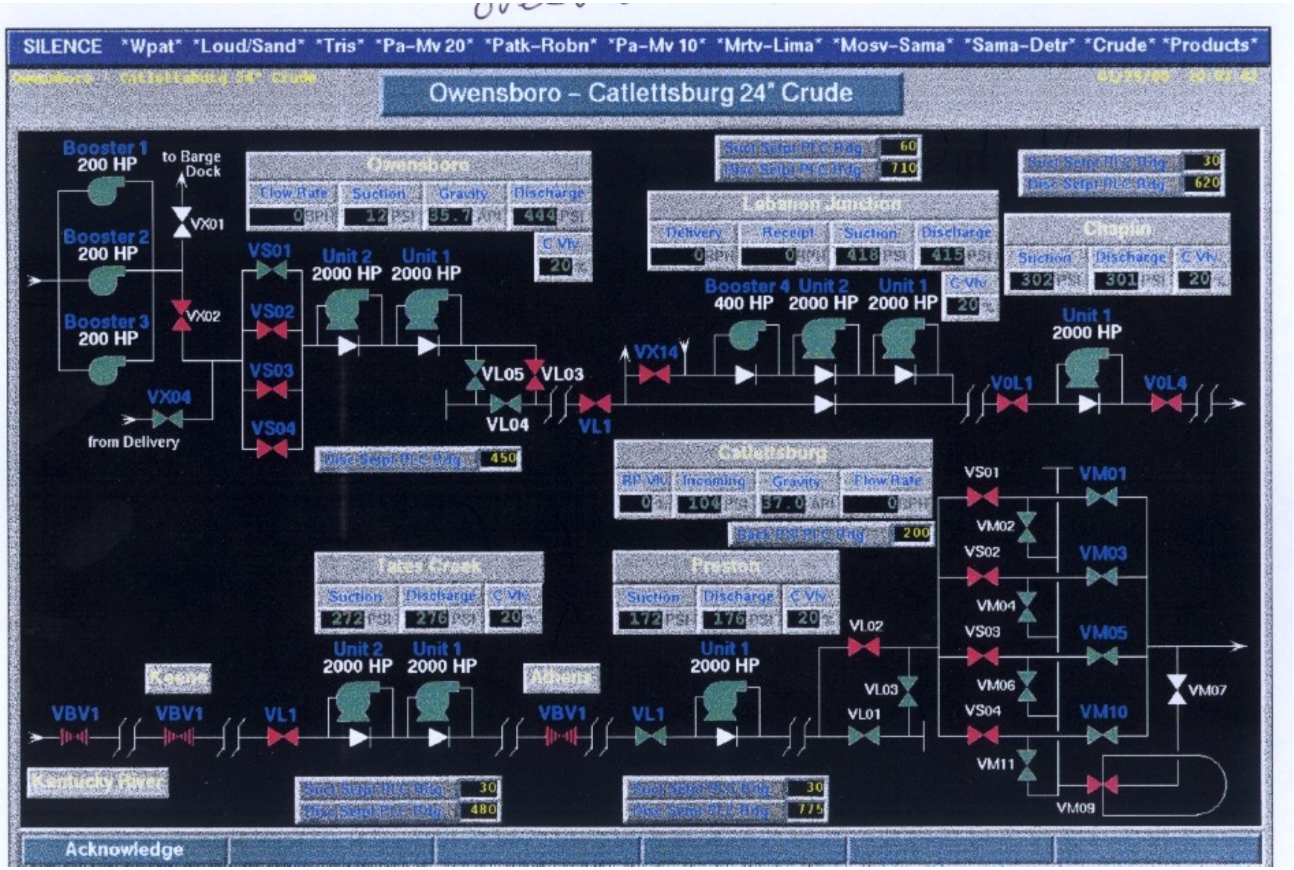
GPS Display

Pipeline Control System

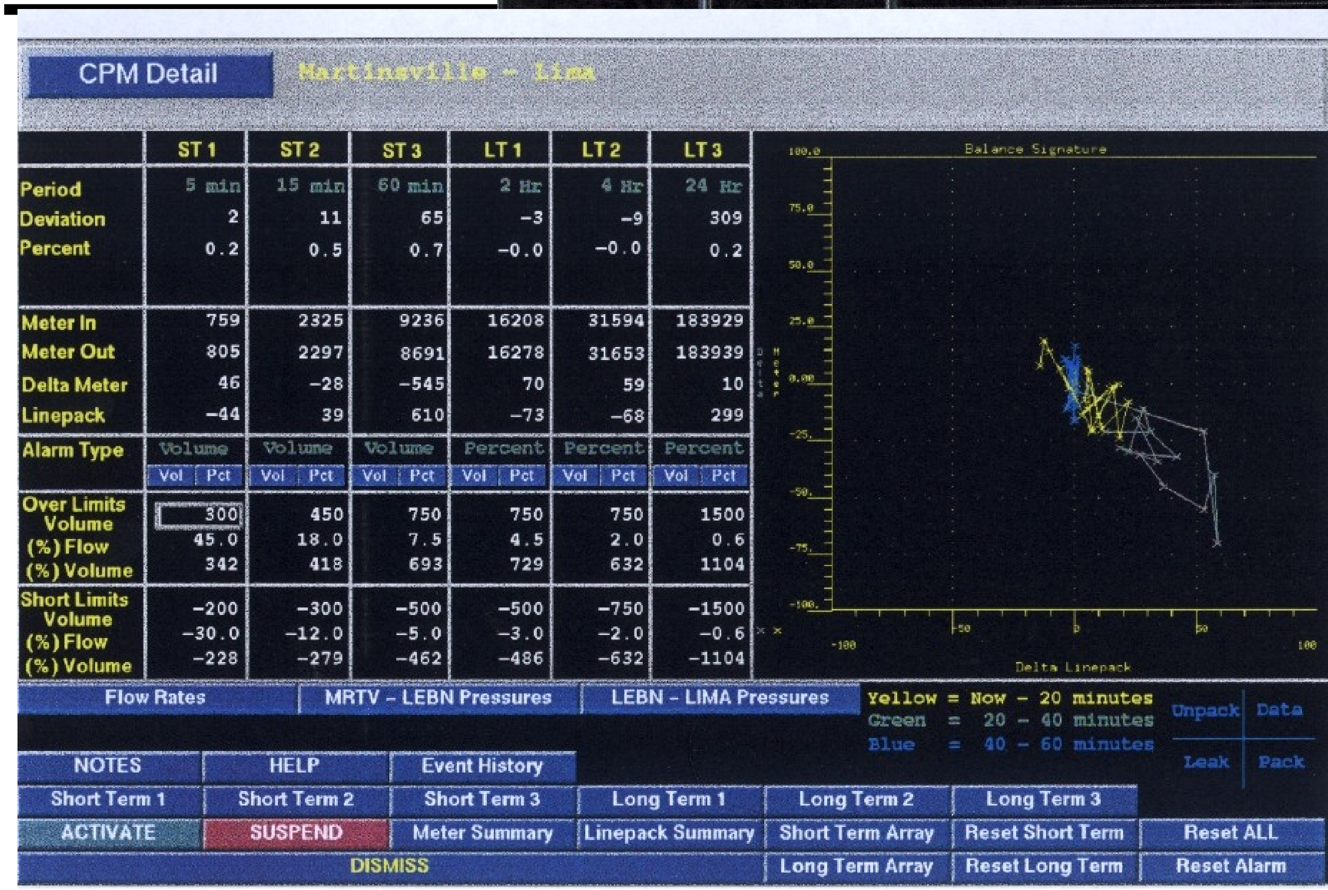
SCADA System



Process Control Screen




SILENCE -Rocky Mountain -Gulf Coast Products -Gulf Coast Crude -Midwest Products -Midwest Crude -Kentucky -Ohio
General Alarm Summary
Tank 5 - Chatham 8" Crude
01/29/00 10:29:19
Page: 1
Goto Top
Date/Time
Group
Alarm Description
01/29/00 10:00:31 TNK5_CHAT_8 Tank 5 - Chatham: PLM - ALARM - 2hr (-436.6), 4hr (-429.6).
01/29/00 09:00:31 CHAT_MAPL Chatham MAPL Station: PLM - ALARM - 2hr (391.3), 4hr (392.4), 24hr (1914.6).
01/29/00 03:00:30 EAST_CAMERON_8 East Cameron - Vermilion: PLM - ALARM - 4hr (NORMAL), 24hr (1548.0).
01/28/00 17:00:31 CSPR_SALS_20 Guernsey Station: PLM - ALARM - 4hr (NORMAL), 24hr (7134.8).
01/26/00 00:43:08 CHAT_CSPR_16 Chatham_PLT: Lockout Unit 5: Change to state ALARM.
Page Acknowledge

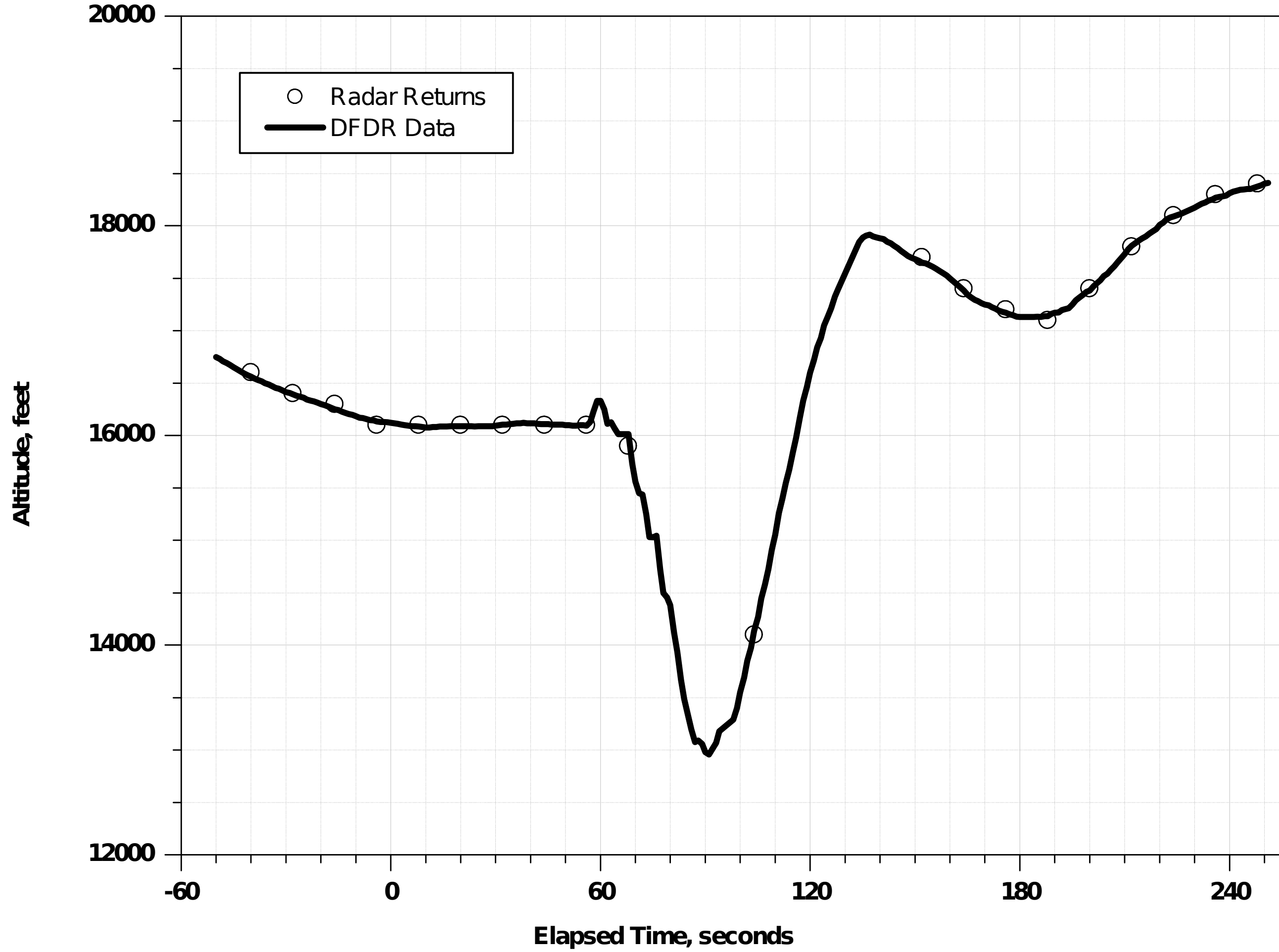

CPM Detail
Martinsville - Lima
ST 1 ST 2 ST 3 LT 1 LT 2 LT 3
Period 5 min 15 min 60 min 2 Hr 4 Hr 24 Hr
Deviation 2 11 65 -3 -9 309
Percent 0.2 0.5 0.7 -0.0 -0.0 0.2
Meter In 759 2325 9236 16208 31594 183929
Meter Out 805 2297 8691 16278 31653 183939
Delta Meter 46 -28 -545 70 59 10
Linepack -44 39 610 -73 -68 299
Alarm Type Volume Volume Volume Percent Percent Percent
Vol Pct Vol Pct Vol Pct Vol Pct Vol Pct Vol Pct
Over Limits Volume 300 450 750 750 750 1500
(%) Flow 45.0 18.0 7.5 4.5 2.0 0.6
(%) Volume 342 418 693 729 632 1104
Short Limits Volume -200 -300 -500 -500 -750 -1500
(%) Flow -30.0 -12.0 -5.0 -3.0 -2.0 -0.6
(%) Volume -228 -279 -462 -486 -632 -1104
Balance Signature
Delta Meter
Delta Linepack
Flow Rates
MRTV - LEBN Pressures
LEBN - LIMA Pressures
Yellow = Now - 20 minutes
Green = 20 - 40 minutes
Blue = 40 - 60 minutes
Unpack Data
Leak Pack
NOTES HELP Event History
Short Term 1 Short Term 2 Short Term 3 Long Term 1 Long Term 2 Long Term 3
ACTIVATE SUSPEND Meter Summary Linepack Summary Short Term Array Reset Short Term Reset ALL
DISMISS Long Term Array Reset Long Term Reset Alarm

A300-600 Inflight Upset

Event Sequence

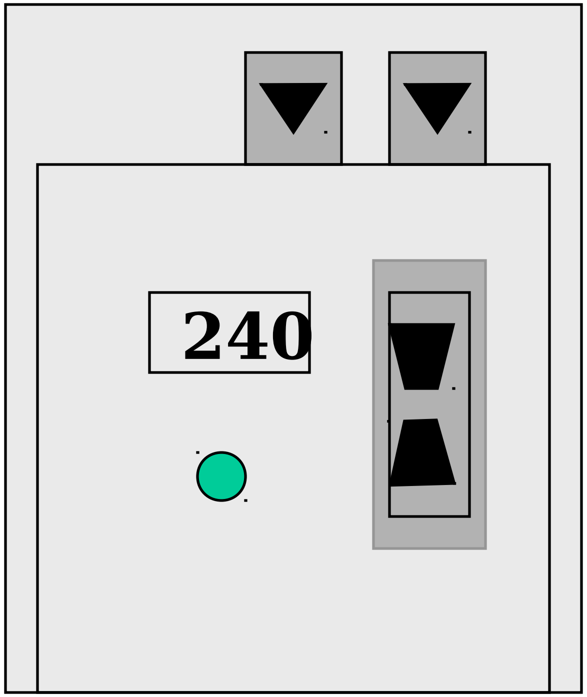
- Autothrottle set to hold 210 knots
- Engaged at start of descent from FL240
  - During descent - power reduced from idle to mechanical stops
- Not engaged at level off at FL160
- Airspeed decreased
- About 170 knots flightcrew advanced throttles
- Stall warning activated and upset occurred
- No evidence of autothrottle malfunction

AA 903 Altitude Plot



Cockpit

Instrument Diagram



Autothrottle Controls

- Engaged via button on glareshield
- Disengage - depress disconnect button on throttle, FMA to amber “MAN THR”, green bars on FCU out
- Other airplanes have warning systems requiring additional flightcrew action
- A300 - passive and persistent indications
- More typical of information display, does not command attention, possible delay between inadvertent disconnect and recognition

A300 Upset
Loss of Displays

- Primary flight controls went out momentarily during upset
- Replaced by indication that computers driving the displays were undergoing automatic reset and self-test
- Function designed to detect unreliable data - monitors flight parameters

A300 Upset
Loss of Displays

- Reset threshold for roll rate - greater than 40 degrees per second
- Airbus first time reset reported during upset
- Recommendation issued to FAA asking that Airbus modify this software on A300 because of the potential for loss of information during unusual attitude recovery

What do these accidents tell us?

- Role of defaults in adaptive automation
- Effects of high false alarm rates
- Dangers of passive monitoring
- Unanticipated failure modes

and, that training just won't cover everything